

# 信息物理系統安全 Cybersecurity for Cyber-Physical Systems

林有立 博士

新科工程網絡安全首席技術官

March 2024

## What is Cyber-Physical System? **信息物理系統的定義**

- The term “cyber-physical systems” was coined more than 15 years ago, but it is now entering the mainstream as digital transformation intensifies, and operational technology (OT) environments become increasingly interconnected with IT systems and Internet of Things (IoT) devices.

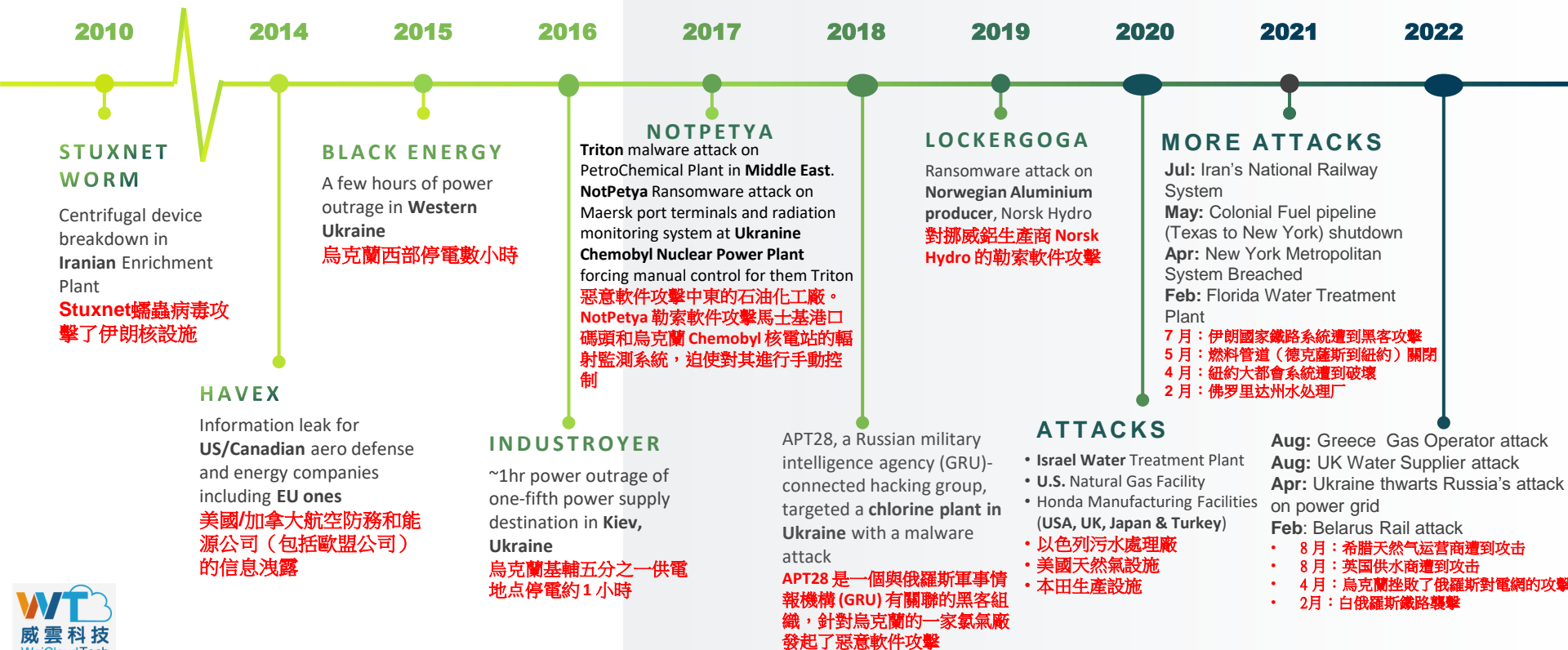
**“信息物理系統”一詞是在15年前創造的，但隨著數字化轉型的加劇以及工業系統 (OT) 環境與 IT 系統和物聯網 (IoT) 設備的互連日益緊密，現在正成為主流。**

- Cyber-physical systems encompass OT assets and systems, along with a proliferation of connected devices. As a result, when we think about protecting OT environment, we need to start thinking of cyber-physical systems security more holistically, because it better reflects the reality we operate within today, as our physical world connects more deeply and broadly with our digital world.

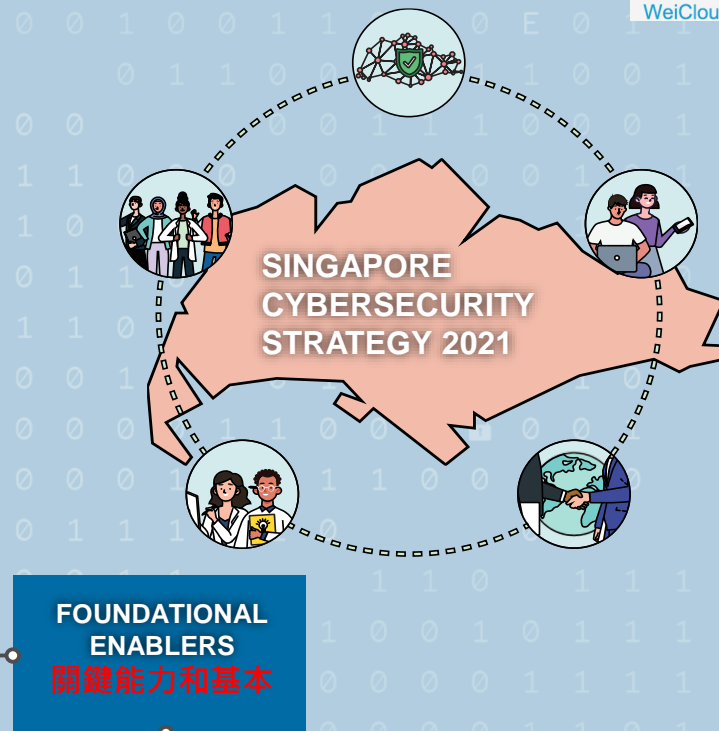
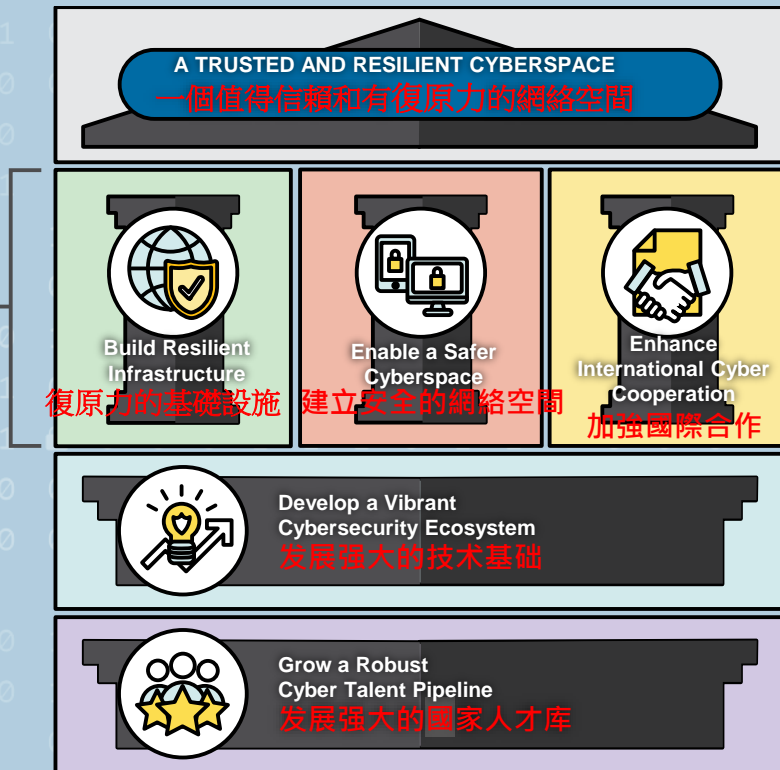
**信息物理系統包括 OT 資產和系統，以及大量連接的設備。因此，當我們考慮保護 OT 環境時，我們需要開始更全面地考慮網絡物理系統安全，因為它更好地反映了我們當今運營的現實，因為我們的物理世界與我們的數碼世界聯繫得更深入、更廣泛。**

# Increasing Cyber Threats – Real & Imminent 日益嚴重的網絡威脅

## OT System 工業控制系統



# National Level 國家網絡安全戰略 – Cyber Security Agency (CSA) has formulated the cybersecurity strategy and is coordinating across the 11 critical sectors in national cyber defence



## CSA Guidelines

- Feb 2018: CSA Cybersecurity Act, 網絡安全法案
- Oct 2019: OT Cybersecurity Masterplan (latest), 工控系統網絡安全總體規劃
- Dec 2019: OT Cybersecurity Code of Practice Version 1.0, 實務守則 1.0
- July 2022: OT Cybersecurity Code of Practice Version 2.0, 實務守則 2.0

# Securing Critical Information Infrastructures

## 保護關鍵基礎設施




**Government**  
政府部門

Government Buildings  
政府大樓




**Security & Emergency**  
安全和緊急情況

Border Checkpoint  
邊境檢查站  
Police 警務  
Fire & Rescue 消防與救援




**Aviation**  
航空

Airport 機場  
Cargo Terminal 貨運站




**Maritime**  
海事

Port Terminals 港口碼頭  
Bunker 掩體



**Infocomm**  
資信通訊

Data Centre 數據中心  
Telco 電訊公司



**Land Transport**  
陸路交通

Railway 鐵路  
Traffic Lights 交通管理



**Healthcare**  
醫療保健

Hospital 醫院  
Medical Centre 醫療中心



**Water**  
水利

Water Treatment Plant  
污水處理廠  
Barrage & Dam 攔河壩



**Energy**  
能源

Power Plant 發電廠  
Substation 變電站  
Gas Work 氣體工作



**Finance**  
金融

Stock Exchange 股票交易  
Central Bank & Banks  
銀行



**Media**  
媒體

Newspaper 新聞  
Broadcasting Station 電台

# OT Cybersecurity Code of Practice Version 2.0 實務守則 2.0

4 July 2022

Issuance of OT Cybersecurity  
Code of Practice Version 2.0  
實務守則 2.0發行日

4 July 2023

In Compliance by  
實務守則 2.0合規日

## Main Differences 主要區別

- One of the Board of Director must be Cybersecurity trained 其中一名董事會成員必須接受過網絡安全培訓
- Access Control, implement solution with auto logout after detection of inactivity 接入控制, 自動退出程序
- Implement Database Security and monitoring on OT System 在工控網絡系統上實施數據庫安全和監控
- Implement Domain Name System Security Extension (DNSSEC) 實施域名系統安全擴展管理
- Isolate affected network segments of the CII in the event of a cybersecurity incident 在發生網絡安全事件時  
隔離關鍵信息通信基礎設施受影響的網段
- Threat Hunting capability 威脅掃描和響應能力
- Cyber Threat Intelligence and Information Sharing 威脅情報、數據和信息共享
- Annual Cybersecurity Exercise 年度網絡安全演習
- Compulsory Cybersecurity Training and Skills development 人員進行網絡安全教育、技術培訓和技能考核

# Challenges and Pain Points in OT Environment

## 工控系統面臨的挑戰和痛點



VAPT are manual, tedious and based on Interview

**VAPT 是人工作業，繁雜並且基於面試**



Unable to map out threats to assets effectively

**無法有效描繪工控系統資產面臨的威脅**



Information gap between ICS (OT) and Cybersecurity staff

**ICS (OT) 與網路安全人員之間的資訊差距**



Threat intel from various sectors and domains not relevant to sector & region

**來自與部門和地區無關的各個部門和領域的威脅情報**



Determining and aligning business processes

**確定和調整業務流程**



Adhering to IEC62443 Standards and Compliance

**國際標準和合規性**



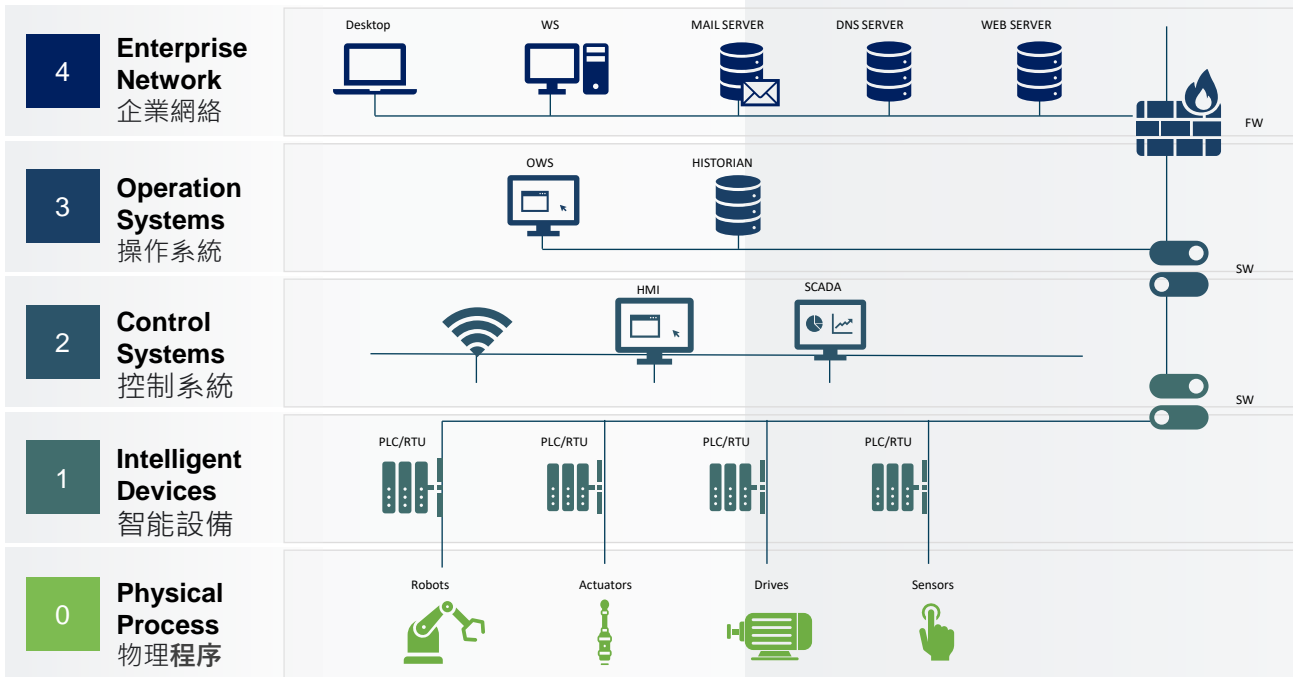
Adhering to CSA Cybersecurity Code of Practice 2.0 Compliance

**遵守網路安全局網路安全行為準則 2.0**

# OT Security Solution Coverage 解決方案

## Leveraging the Purdue model Purdue 模式的應用

### LEVELS



4級: 包括企業資源規劃 (ERP) 軟件、數據庫、電子郵件服務器和其他管理製造運營物流並提供通信和數據存儲的系統。該網絡從 ICS 系統收集數據用於業務決策。

3級: 支持生產工作流程的管理。示例包括批次管理、製造運營管理/製造執行系統 (MOMS/MES) 和數據歷史記錄。

2級: 是控制系統內整個過程的設備。例如，人機界面 (HMA) 和 SCADA 軟件使人能夠監控和管理流程。

1級: 由監控級別 0 的設備並向其發送指令的系統組成。示例包括可編程邏輯控制器 (PLC)、遠程終端單元 (RTU) 和智能電子設備 (IED)。

0級: 包括物理組件。這包括電機、泵、傳感器、閥門等

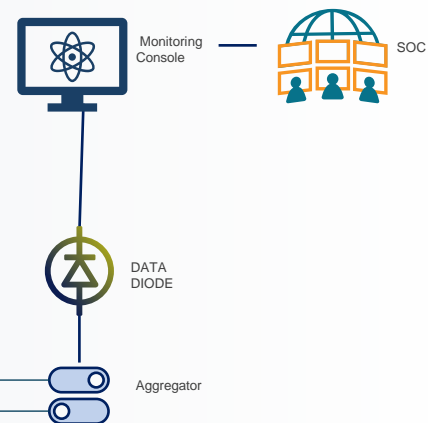


# OT Security Solution Coverage, 解決方案

## IT/OT Integration IT/OT 整合

### LEVELS

- 4 **Enterprise Network**  
企業網絡
- 3 **Operation Systems**  
操作系統
- 2 **Control Systems**  
控制系統
- 1 **Intelligent Devices**  
智能設備
- 0 **Physical Process**  
物理程序



# Use Case for Railway Transport

## 鐵路方案

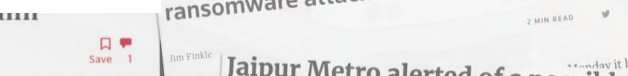
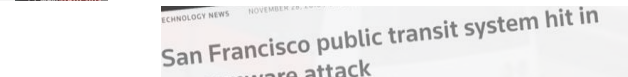
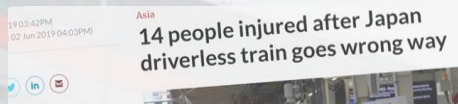
# Cyber Threat Landscape of Train Operators

## 鐵路運營商的網絡威脅態勢

The complexity, dynamics and size of rail networks create an environment that is difficult to monitor effectively; moreover, increasing rail connectivity leaves them extremely vulnerable

鐵路網絡的複雜性、動態性和規模創造了一個環境難以有效監控；此外，增加鐵路連通性使系統極度脆弱

- ★ Cybersecurity breaches may lead to service disruptions, data breaches, derailments, network outages, and more  
網絡安全漏洞可能導致服務中斷、數據洩露、脫軌、網絡中斷等
- ★ Rail companies face legal liability, financial loss, injury, and reputational harm  
鐵路公司面臨法律責任、財務損失、傷害和聲譽損害



# Facing a wide attack surface

## 面對廣泛的攻擊面



信令通訊 Signalling Communication

用於控制鐵路交通移動的系統 System that control the movement of railway traffic.



無線通信 Wireless Communication

遠程控制和更新的系統 Systems that are controlled and updated remotely.



維修渠道 Maintenance Channels

使用不安全的硬件、軟件和與關鍵/SIL4 環境的连接 Use of unsafe hardware, software and connections to the critical/SIL4 environment.



供應鏈 Supply Chain

連接到基礎設施以進行更新和組件安裝 Connection to the infrastructure for update and component installation.



鐵路車輛 Rolling Stock

火車上的扁平網絡拓撲和薄弱的物理安全性 Flat network topology on trains and weak physical security.

# Cybersecurity Operations for Railway Transport in Singapore

## 新加坡鐵路運輸網絡安全運營

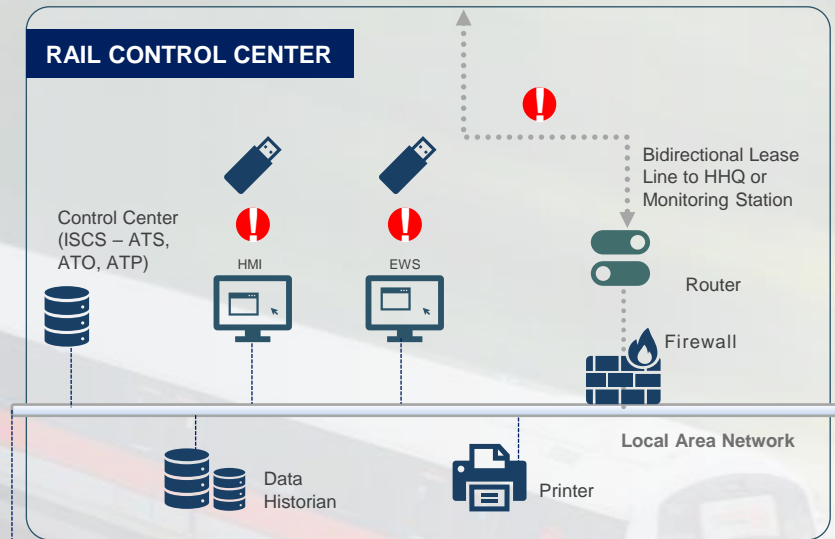
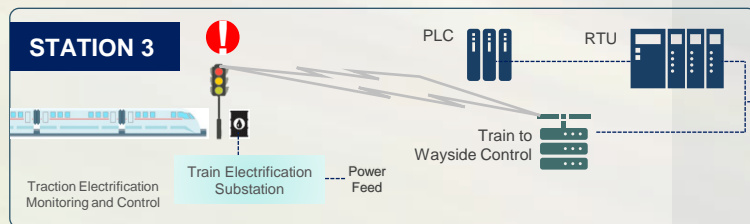


資安監控中心(SOC)  
Cybersecurity Operation  
Centre



# Railway System Potential Intrusion Points

## 地鐵系統潛在的入侵點

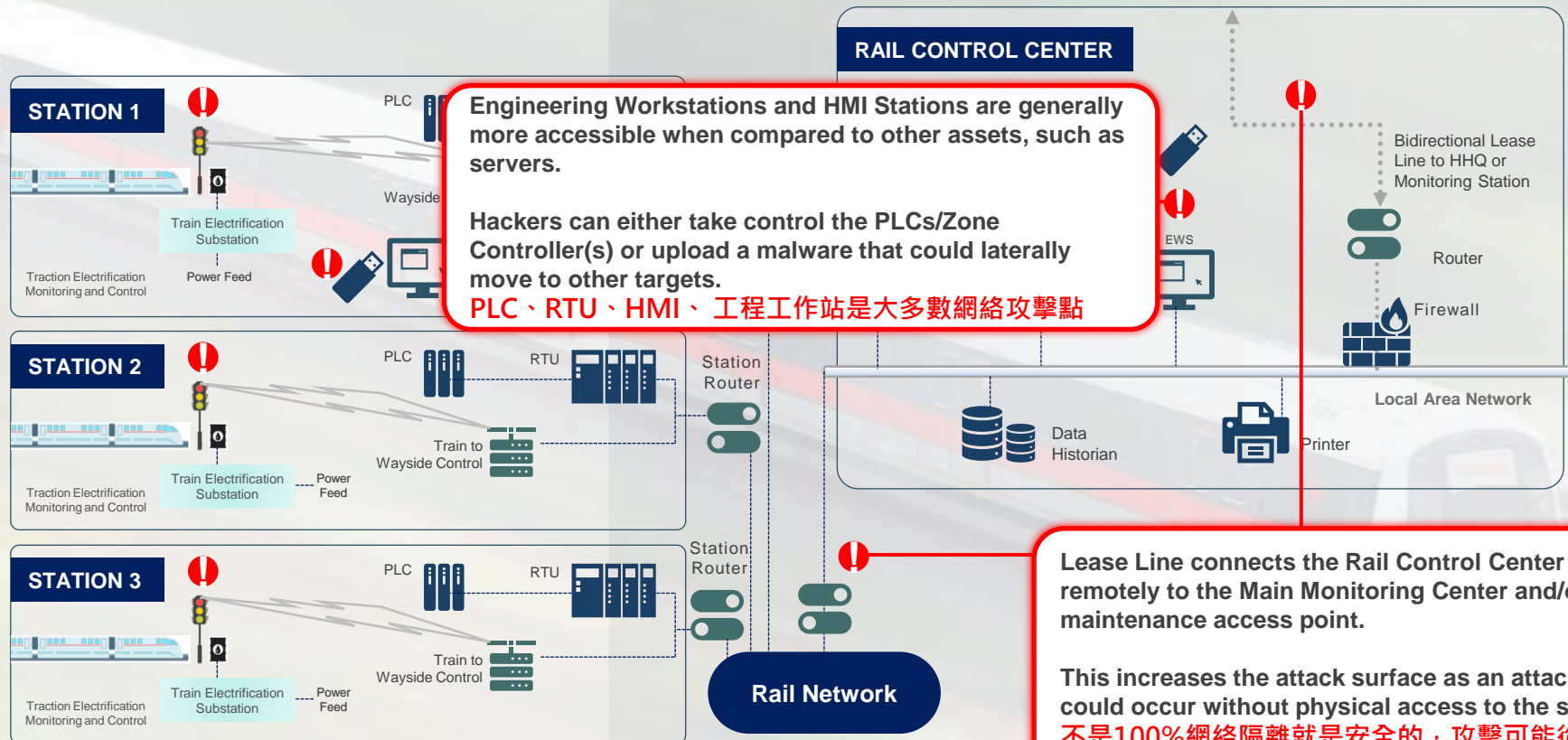


LEGEND

 **VULNERABLE**  
弱点

# Railway System Potential Intrusion Points

## 地鐵系統潛在的入侵點



Engineering Workstations and HMI Stations are generally more accessible when compared to other assets, such as servers.

Hackers can either take control the PLCs/Zone Controller(s) or upload a malware that could laterally move to other targets.

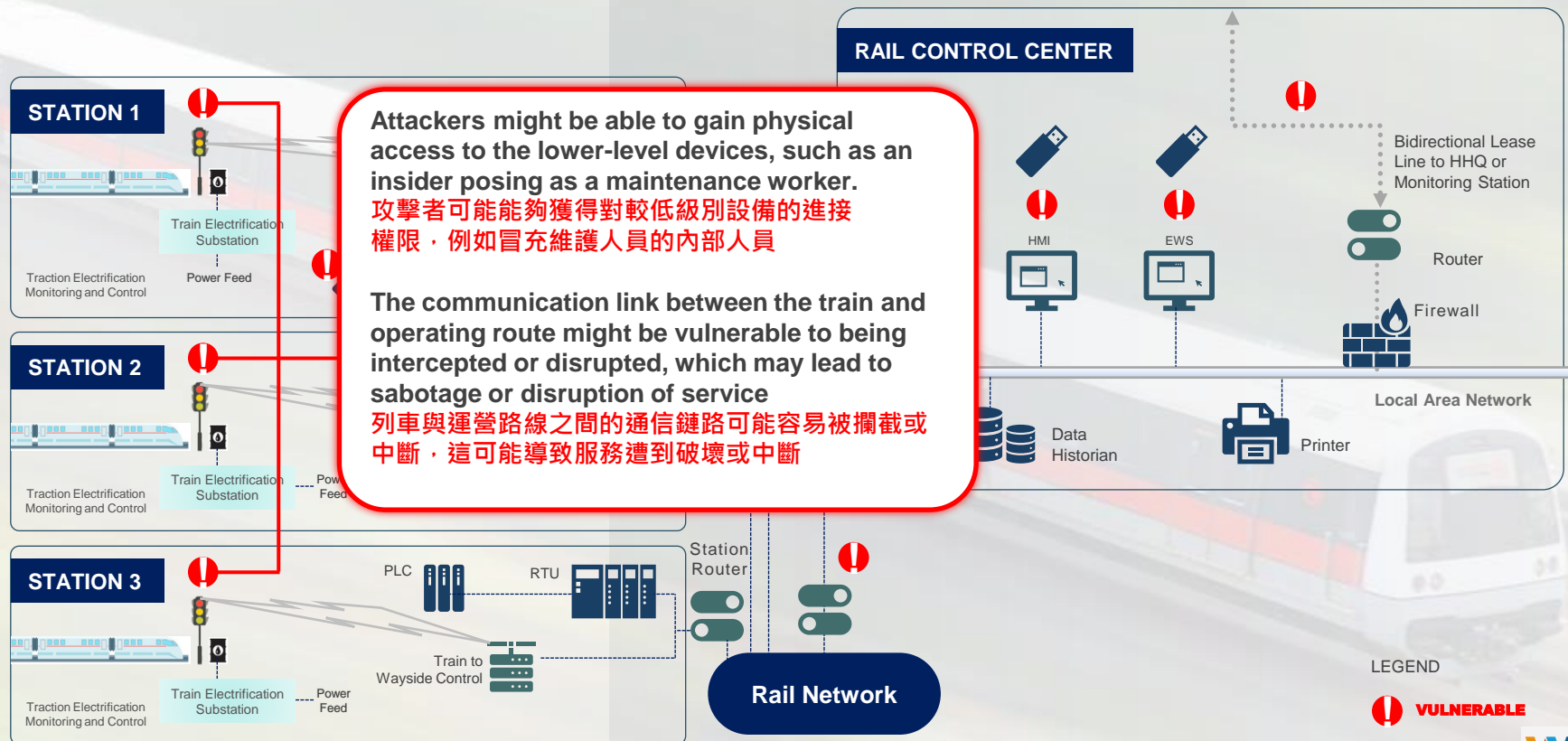
PLC、RTU、HMI、工程工作站是大多數網絡攻擊點

Lease Line connects the Rail Control Center remotely to the Main Monitoring Center and/or maintenance access point.

This increases the attack surface as an attack could occur without physical access to the site.  
不是100%網絡隔離就是安全的，攻擊可能從鐵路交通指揮中心開始進攻

# Railway System Potential Intrusion Points

## 地鐵系統潛在的入侵點

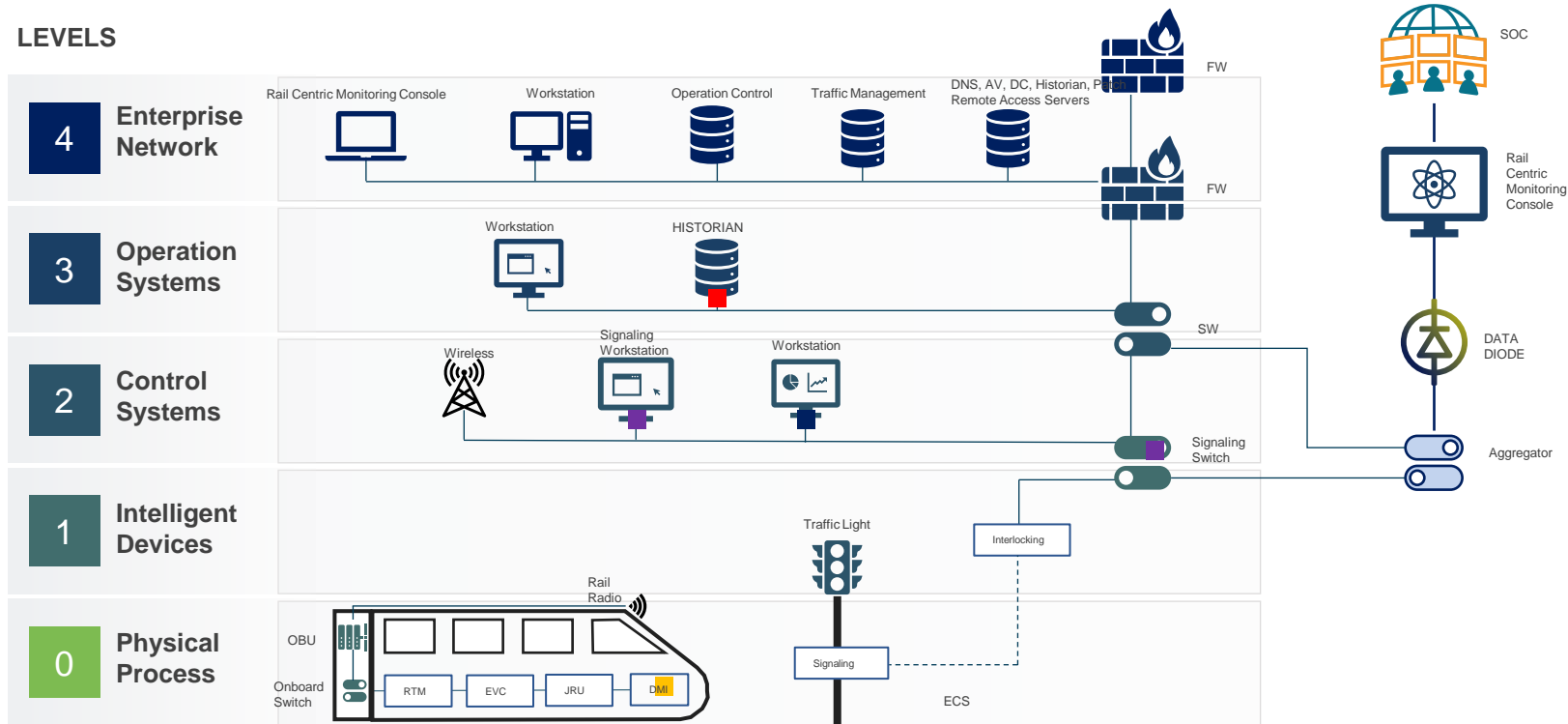




# OT Solutioning Based on Purdue Model

## 基於普渡模型的OT解決方案

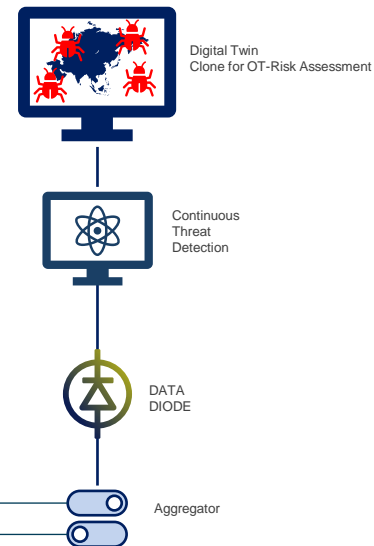
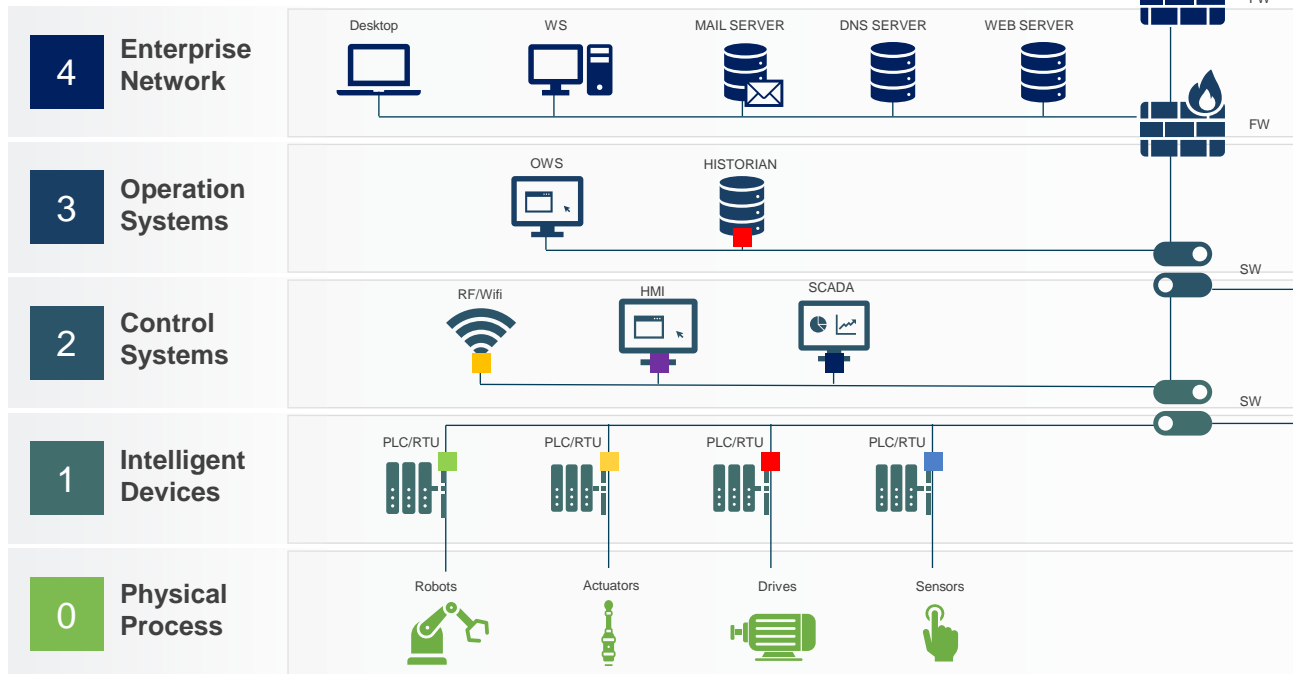
### LEVELS



# Elevating to next level 提升到一個新的水平

## From Reactive to Proactive Approach 從被動到主動

### LEVELS



# CIARA: Industrial Risk Assessment & Management Platform (Proactive Strategy 主動策略)



## 持續的工業風險評估平台

智能探針數據



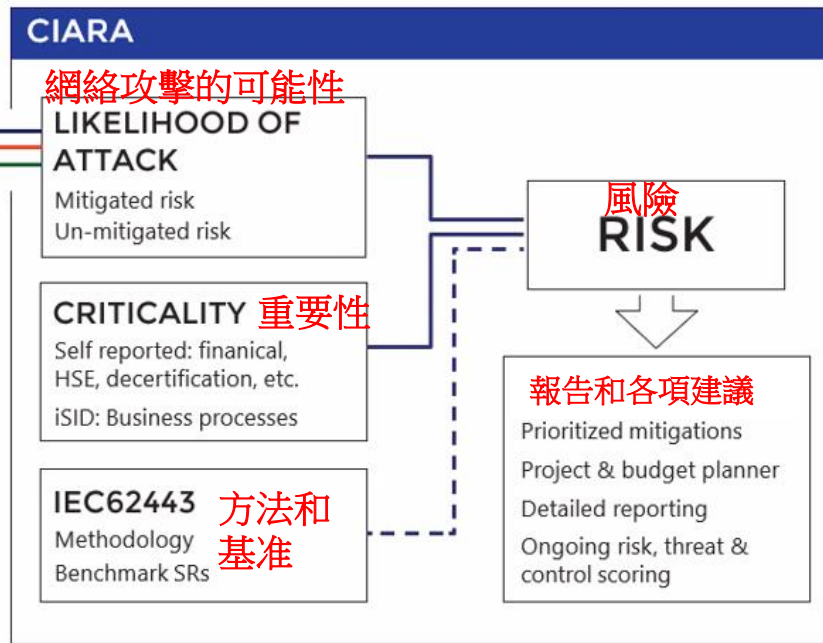
Automatically obtain all data, generates report, identifies all threat intel 自動收集數據,生成報告, 確認所有威脅情報



Fully-automated, data-driven vulnerability assessment engine 完全自動化落點評估



## Solution Workflow 解決方案工作流程



Simulates hundreds of commonly used security controls 模擬數百個常用的安全控制



Utilises variety of sources, modelling network vulnerabilities, defences and possible attacks 利用各種來源, 建模網絡安全漏洞, 網絡防禦, 可能的網絡攻擊

數碼孿生平台  
Digital Twin



# Value Proposition of Continuous OT-Risk Assessment

## 持續 OT 風險評估的價值主張



Automate and simulate top attack scenarios  
24hrs 漏洞並模擬可能的攻擊場景



Map out assets based on region and sector  
基於地區和部門



Close the gap between ICS (OT) vulnerabilities and Cybersecurity Staff  
彌補OT資安漏洞与資安人員之間的差距



Filtering of threat intel based on sector and region  
針對性威脅情報



Determine and align business processes  
協調商業流程以達到企業的目標



IEC62443 Compliance  
確保IEC62443合規性



CCoP v2.0 Compliance  
可根據您的環境進行調節，實現 CCoP v2.0 合規性 (新加坡)

*Staying ahead on Cybersecurity* 在網絡安全方面保持領先

As IT Cybersecurity becomes mature,  
OT network offers an easy target for cybercriminals.

隨著 IT 網絡安全趨向成熟，OT 網絡將會是網絡罪犯的下一個簡單目標。

**Thank you**